重要数据安全风险评估项目采购需求

一、项目概况

为贯彻落实习近平总书记关于网络强国的重要思想、《网络安全法》《数据安全法》《个人信息保护法》《湖南省网络安全和信息化条例》等法律法规的相关要求以及《湖南省自然资源厅网络安全工作责任制实施细则》等文件规定，切实做好我厅重要数据安全防护工作，决定实施重要数据安全风险评估项目，通过漏洞扫描、渗透测试等技术手段，全面排查网络安全隐患，筑牢网络安全屏障。

二、项目预算

18万元。

三、商务需求

因本项目属于重要数据安全风险评估项目，为保证供应商基本的服务能力和服务水平，对供应商的资质等要求如下：

（一）供应商具备中国通信企业协会颁发的通信网络安全服务能力网络安全风险评估一级及以上资质，提供证书复印件并加盖公章。

（二）供应商项目负责人需同时具备高级工程师证书和CISP证书（注册信息安全专业人员），提供项目负责人相关证书复印件、近三个月任意一个月社保证明并加盖公章。

（三）供应商拟任重要数据安全风险评估实施团队成员至少5人（不含项目负责人），团队成员均需具备CISP证书（注册信息安全专业人员），至少一人需持有高级工程师证书或信息系统高级项目管理师（高级）职称，提供项目实施团队成员相关证书复印件、近三个月任意一个月社保证明并加盖公章。

（四）供应商需派驻1名采购人认可的技术人员（非重要数据安全风险评估实施团队成员）进驻项目现场开展驻场服务工作，驻场人员要求熟悉网络安全相关法律法规，需持有CISP证书（注册信息安全专业人员）。工作时间和工作地点由采购人指定，驻现场技术人员因特殊原因需要更换，供应商必须提出书面申请并取得采购人书面回复同意后方可更换，不得擅自撤离驻现场工作人员。本条须出具承诺函并加盖供应商公章。提供拟投入本项目人员相关证书复印件及竞价截止前三个月任意一个月缴纳社保证明。

四、服务内容及要求

依据相关规范标准对授权的互联网资产开展重要数据安全风险评估4次，共出具检查报告4份，并提供具体的漏洞修复建议。

具体服务内容如下：

| **序号** | **服务子项** | **服务内容** | **数量** |
| --- | --- | --- | --- |
| 1 | 重要数据安全风险评估 | 经授权后，通过模拟黑客的攻击行为与分析方法对指定范围内的内网、外网重要应用系统进行人工渗透测试，识别目标系统中存在的安全隐患，提供修复建议并指导漏洞修复工作。同时，针对整改情况提供复测服务。 | 4次 |

五、服务原则

1.符合性原则：遵循国家、行业和组织相关的安全技术规范要求。

2.规范性原则：工作过程和文档交付具有规范的操作流程，内容明确，责任清晰，可以便于项目的跟踪和控制。

3.整体性原则：提供整体、全面的安全服务，包括业务、应用、系统、网络、管理制度、人员等各个层面和系统规划、设计、建设、入网、运维、退网等各个环节。

4.最小影响原则：服务的实施过程尽可能小的影响系统和网络的正常运行，不能对系统的运行和业务的正常提供产生显著影响（包括系统性能明显下降、网络拥塞、服务中断等），如无法避免出现这些情况需要提前详细描述。

5.保密原则：对项目实施过程中所涉及的数据及信息严格保密，未经授权不泄露给任何单位和个人，不利用此数据进行任何侵害用户网络的行为，项目完成后清除相关文档信息。

六、需满足的服务标准、期限等要求

（一）服务标准：

1、GB/T 33561-2017 信息安全技术 安全漏洞分类

2、GB/T 28458-2012 信息安全技术 安全漏洞标识与描述规范

3、GB/T 30276-2013 信息安全技术 信息安全漏洞管理规范

4、GB/T 30279-2013 信息安全技术 安全漏洞等级划分指南

5、GB/T 20984-2022信息安全技术 信息安全风险评估方法

6、GB/T 24364-2023信息安全技术 信息安全风险管理实施指南

（二）施工工期和服务地点要求

施工工期：合同签订后一年内根据甲方要求开展重要数据安全风险评估4次，并提供相应检查报告。

服务地点：采购人指定地点。

（三）付款方式及付款条件

付款方式：国库集中支付

付款条件：

签订合同后十五个工作日内支付合同总金额40%启动经费；完成安全风险评估并出具相应成果报告，经采购人验收合格后，支付剩余60%合同款。

**采购需求所有条款，供应商需在响应文件中逐一全部响应并加盖公章，否则视为无效响应。**